Ann. Telecommun. (2014) 69:345–346
DOI 10.1007/s12243-014-0434-7

EDITORIAL

Network forensics and challenges for cybersecurity

Wojciech Mazurczyk · Krzysztof Szczypiorski · Hui Tian

Published online: 27 March 2014

1 Introductory remarks

Societies in the contemporary world are becoming more and more dependent on open networks such as the Internet where commercial activities, business transactions, and government services are realized. This has led to the fast development of new cyber threats and information security issues, which are utilized by cyber criminals. Mistrust for telecommunications and computer network technologies have tremendous socio-economic impacts on global enterprises as well as individuals.

Moreover, the occurrence of international frauds often requires the investigation of facts that cross international borders. They are also often subject to different jurisdictions and legal systems. The increased complexity of the communication and networking infrastructure is making investigation of the crimes difficult. Clues of illegal digital activities are often buried in large volumes of data that are hard to inspect in order to detect crimes and collect evidence.

This poses new challenges for law enforcement and forces computer societies to utilize digital forensics to combat the growing number of cybercrimes. Forensic professionals need to be fully prepared in order to be able to provide effective evidence. To achieve these goals forensic techniques must keep pace with new technologies. That is why the field of digital forensics is becoming more and more important for law enforcement and information and network security. Network forensics is a newly emerged research area, and its importance has attracted a great attention among computer professionals, law enforcers, and practitioners. It is a multidisciplinary area that includes multiple fields, i.e., law, computer science, finance, networking, data mining, and criminal justice. However, network forensics still faces diverse challenges and issues in terms of the efficiency of digital evidence processing and the related forensic procedures.

In this special issue, we are delighted to present a selection of ten papers, which, in our opinion, will contribute to the enhancement of knowledge in network forensics and cybersecurity. The collection of high-quality research papers provides a view on the latest research advances on special security incidents, steganography, and steganalysis.

In the first paper [1], Dohoon Kim, Jungbean Lee, Young-Gab Kim, Byungsik Yoon, and Hoh Peter propose an architecture for IMS/SIP-based lawful interception in wireless 3G networks and original techniques of interception, where content service providers are separated from network providers. The authors present the results of a Quality of Service performance analysis conducted on their proposed interception architecture for various numbers of IMS users.

The authors of the second paper [2], Robert Filasiak, Maciej Grzenda, Marcin Luckner, and Pawel Zawistowski, introduce a new way of testing methods detecting network threats, including a procedure for creating realistic reference data sets describing network threats and the processing and use of these data sets in testing environments. The new approach is evaluated on the basis of the problem of spam detection, and two measures, accuracy and performance of threat detection, are considered.

Bo-Chao Cheng, Guo-Tan Liao, Hsu-Chen Huang, and Ping-Hai Hsu in their paper [3] propose a new mechanism to overcome the disadvantage of requiring huge data storage for network forensics analysis tools for denial-of-service attacks. The experimental results confirmed that the proposed mechanism, based on advanced training methods to build proper data classifiers, is useful in reduction of data quantity.

W. Mazurczyk (✉) · K. Szczypiorski
Warsaw University of Technology, Warsaw, Poland
e-mail: wmazurczyk@tele.pw.edu.pl

K. Szczypiorski
e-mail: ksz@tele.pw.edu.pl

H. Tian
National Huaqiao University, Huaqiao, China
e-mail: hian@hqu.edu.cn

In the next paper [4] by Tsu-Yang Wu, Tung-Tso Tsai, Yuh-Min Tseng, the public key encryption services with keyword search are considered. The new scheme is proposed for the special type of these services with a designated server and with the removed requirement of possessing the secure channel. The scheme is fully evaluated and seems to be resistant for known attacks with better performance in terms of computational time.

Weiwei Liu, Guangjie Liu, and Yuewei Dai in [5] present the new focus on a relationship between syndrome coding for minimizing additive distortion and maximum likelihood decoding for linear codes to analyze the main parameters of convolutional codes, which influence the embedding efficiency. Experimental results show that presented solution achieve the reduced time complexity and storage requirement meanwhile than other methods from state of the art.

"Hidden and Under Control" is main topic of the next paper [6] authored by Steffen Wendzel and Joerg Keller. In this survey, the first overview and categorization of existing micro protocols, i.e., protocols to enhance network covert channels by adding headers to the hidden payload, is made. The paper includes analysis of micro protocol features and presents currently uncovered research directions for these protocols. Finally, the authors propose the significant improvement to this field by optimization of the invisibility of micro protocols.

In the seventh paper in this special issue, Fengyong Li, Xinpeng Zhang, Jiang Yu, and Wenfeng Shen [7] show an adaptive steganographic scheme in JPEG images by design of new distortion function. This function is derived from both the coefficient residual and coefficient value, which measures the risks of detection due to the modification on cover data. The experimental results demonstrate that the steganographic security is significantly improved by this function.

Xinpeng Zhang, Chuan Qin, and Liquan Shen in [8] propose an efficient data hiding scheme for wet paper channel by using a multilayer construction, in which a number of node-bits in different layers are derived from all cover bits and used to carry the secret data. An equilibration mechanism is also introduced in the paper to flip the denser changeable cover bits with higher probability.

Artur Janicki, Wojciech Mazurczyk, and Krzysztof Szczypiorski in [9] address the issue of steganalysis of TranSteg (Trancoding Steganography). Various TranSteg scenarios and possibilities of warden(s) localization are analyzed with regards to the TranSteg detection. A novel steganalysis method based was developed by authors and tested for various codec pairs in a single wardenscenario with double transcoding.

Finally, the last paper [10] by Songbin Li, Haojiang Deng, Hui Tian, and Qiongxing Dai contains an analysis of characteristics in intra-frame coding caused by modulating intra prediction modes for information hiding and the proposal of statistical models corresponding to the correlation of prediction modes to make quantitative extraction of these correlation characteristics. The detector was constructed based on the support vector machine and used to show that the mean of the detection accuracy, recall ratio, and precision ratio are all excellent for different test video sequences.

We believe that this special issue will contribute to enhancing knowledge in many diverse areas of the ICT security. In addition, we also hope that the presented results will stimulate further research in the important areas of information and network security, including network forensics and challenges for cybersecurity.

Acknowledgement This research was partially supported by the Polish National Science Center under grant no. 2011/01/D/ST7/05054 and Natural Science Foundation of China under Grant No. 61302094.

References

1. Dohoon Kim, Jungbean Lee, Young-Gab Kim, Byungsik Yoon, Hoh Peter In: 3G IP multimedia subsystem based framework for lawful interception, Annals of Telecommunications, this issue.
2. Robert Filasiak, MaciejGrzenda, MarcinLuckner, PawelZawistowski: On the testing of network cyber threat detection methods on spam example, Annals of Telecommunications, this issue.
3. Bo-Chao Cheng, Guo-Tan Liao, Hsu-Chen Huang, Ping-Hai Hsu: CHEETAH: A space-efficient HNB-based NFAT approach to supporting network forensics, Annals of Telecommunications, this issue.
4. Tsu-Yang Wu, Tung-Tso Tsai, Yuh-Min Tseng: Efficient searchable ID-based encryption with a designated server, Annals of Telecommunications, this issue.
5. Weiwei Liu, Guangjie Liu, Yuewei Dai: Syndrome Trellis codes based on minimal span generator matrix, Annals of Telecommunications, this issue.
6. Steffen Wendzel, Joerg Keller: Hidden and Under Control. A survey and outlook on covert channel-internal control protocols, Annals of Telecommunications, this issue.
7. Fengyong Li, Xinpeng Zhang, Jiang Yu, Wenfeng Shen: Adaptive JPEG steganography with new distortion function, Annals of Telecommunications, this issue.
8. Xinpeng Zhang, Chuan Qin, Liquan Shen: Efficient wet paper embedding for steganography with multi-layer construction, Annals of Telecommunications, this issue.
9. Artur Janicki, Wojciech Mazurczyk, Krzysztof Szczypiorski: Steganalysis of transcoding steganography, Annals of Telecommunications, this issue.
10. Songbin Li, Haojiang Deng, Hui Tian, Qiongxing Dai: Steganalysis of prediction mode modulated data-hiding algorithms in H.264/AVC video stream, Annals of Telecommunications, this issue.